WHAT IS CLAIMED IS:

1. A method of authenticating a hardware token, comprising the steps of:

generating a host fingerprint F;

transmitting the fingerprint to an authorizing device;

receiving a random value R from the authorizing device;

computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;

transmitting the challenge R' to the hardware token;

receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and

transmitting the response X to the authorizing device.

2. The method of claim 1, wherein the step of generating the fingerprint comprises the steps of:

collecting host information C; and

forming the fingerprint F at least in part from the host information C.

3. The method of claim 2, wherein the step of forming the fingerprint F from the host information C comprises the step of hashing the host information C.

4. The method of claim 2, wherein:

the method further comprises the step of receiving authorizing device specific value V; and

the step of forming the fingerprint F at least in part from the host information C comprises the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

5. The method of claim 4, wherein the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the step of forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

6. The method of claim 4, wherein the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the step of forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

7. The method of claim 2, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

processor serial number;
hard drive serial number;
network interface MAC address;
BIOS code checksum;
operating system; and
system directory timestamp.

8. The method of claim 1, further comprising the step of:

receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

9. The method of claim 1, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

10. The method of claim 9, wherein the response X is the challenge R' encrypted by the shared secret S.

11. The method of claim 1, wherein the response X is generated from a private key K_{pr} of a of a key pair having the private key K_{pr} accessible to the token and a public key K_{pu} accessible to the authorizing device.

12. An apparatus for authenticating a hardware token, comprising:

means for generating a host fingerprint F;

means for transmitting the fingerprint to an authorizing device;

means for receiving a random value R from the authorizing device;

means for computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;

means for transmitting the challenge R' to the hardware token;

means for receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and

means for transmitting the response X to the authorizing device.

13. The apparatus of claim 12, wherein the means for generating the fingerprint comprises:

means for collecting host information C; and

means for forming the fingerprint F at least in part from the host information C.

14. The apparatus of claim 13, wherein the means for forming the fingerprint F from the host information C comprises means for hashing the host information C.

15. The apparatus of claim 13, wherein:

the apparatus further comprises means for receiving authorizing device specific value V; and

the means for forming the fingerprint F at least in part from the host information C comprises means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

16. The apparatus of claim 15, wherein the means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises means for forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

17. The apparatus of claim 15, wherein the means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the means for forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

18. The apparatus of claim 13, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

processor serial number;
hard drive serial number;
network interface MAC address;
BIOS code checksum;
operating system; and
system directory timestamp.

19. The apparatus of claim 12, further comprising:

means for receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

20. The apparatus of claim 12, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

21. The apparatus of claim 20, wherein the response X is the challenge R' encrypted by the shared secret S.

22. The apparatus of claim 12, wherein the response X is generated from a private key K_{pr} of a key pair having the private key K_{pr} accessible to the token and a public key K_{pu} accessible to the authorizing device.

23. A computer for authenticating a hardware token, the computer having a processor communicatively coupled to a memory storing instructions for performing steps of:

generating a host fingerprint F;

transmitting the fingerprint to an authorizing device;

receiving a random value R from the authorizing device;

computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;

transmitting the challenge R' to the hardware token;

receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and

transmitting the response X to the authorizing device.

24. The apparatus of claim 23, wherein the instructions for generating the fingerprint comprise instructions for performing steps of:

collecting host information C; and

forming the fingerprint F at least in part from the host information C.

25. The apparatus of claim 24, wherein the instructions for forming the fingerprint F from the host information C comprise instructions for hashing the host information C.

26. The apparatus of claim 24, wherein:

the computer further receives an authorizing device specific value V; and

the instructions for forming the fingerprint F at least in part from the host information C comprise instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

27. The apparatus of claim 26, wherein the instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprise instructions for forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

28. The apparatus of claim 26, wherein the instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprise instructions for forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

29. The apparatus of claim 24, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

processor serial number;
hard drive serial number;
network interface MAC address;
BIOS code checksum;
operating system; and
system directory timestamp.

30. The apparatus of claim 23, wherein the instructions further comprise:

instructions for receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

31. The apparatus of claim 23, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

32. The apparatus of claim 31, wherein the response X is the challenge R' encrypted by the shared secret S.

33. The apparatus of claim 23, wherein the response X is generated from a private key K_{pr} of a of a key pair having the private key K_{pr} accessible to the token and a public key K_{pu} accessible to the authorizing device.

34. A method of authenticating a hardware token for operation with a host, comprising the steps of:

retrieving a value X from a memory accessible to an authenticating entity, the value X generated from a fingerprint F of the host and an identifier P securing access to the token;

generating the identifier P at least in part from the value X and the fingerprint F; and

transmitting the identifier P to the token.

35. The method of claim 34, wherein the host fingerprint F is computed at least in part from host information C.

36. The method of claim 34, wherein the host fingerprint F is computed at least in part from host information C and a server specific value V.

37. The method of claim 34, wherein the host fingerprint F is computed at least in part from host information C, a server specific value V and a fixed string Z.

38. The method of claim 34, wherein the value X is computed in the token.

39. The method of claim 34, wherein the value X is computed according to $X = f(P,F)$, wherein $f(P,F)$ is a reversible function such that $f(f(P,F),F) = P$

40. The method of claim 39, wherein $f(P,F)$ comprises P XOR F.

41. The method of claim 34, wherein the value X is further computed at least in part from a user identifier U.

42. The method of claim 41, wherein the value X is computed according to $X = f(P,U,F)$, wherein $f(P,U,F)$ is a reversible function such that $f(f(P,U,F),U,F) = P$.

43. The method of claim 42, wherein $f(\mathrm{P},\mathrm{U},\mathrm{F})$ is P XOR U XOR F.

44. The method of claim 34, wherein:

the authorizing entity is a host computer communicatively coupleable to the token; and

the value X is stored in the host computer.

45. The method of claim 34, wherein the value X is stored in a memory accessible to the authentication entity by performing steps comprising the steps of:

computing a reference value H associated with the value X; and

associably storing the value X and the reference value H in a memory of the token.

46. The method of claim 45, wherein the step of retrieving the value X comprises the steps of:

computing the reference value H at least in part from the fingerprint F; and

retrieving the value X associated with the reference value H.

47. The method of claim 46, wherein the step of computing the reference value H at least in part from the fingerprint F comprises the step of computing H as a hash of the fingerprint F.

48. The method of claim 45, wherein the reference value H is computed at least in part from a hash of the fingerprint F.

49. An apparatus for authenticating a hardware token for operation with a host, comprising:

means for retrieving a value X from a memory accessible to an authenticating entity, the value X generated from a fingerprint F of the host and an identifier P securing access to the token;

means for generating the identifier P at least in part from the value X and the fingerprint F; and

means for transmitting the identifier P to the token.

50. The apparatus of claim 49, wherein the host fingerprint F is computed at least in part from host information C.

51. The apparatus of claim 49, wherein the host fingerprint F is computed at least in part from host information C and a server specific value V.

52. The apparatus of claim 49, wherein the host fingerprint F is computed at least in part from host information C, a server specific value V and a fixed string Z.

53. The apparatus of claim 49, wherein the value X is computed in the token.

54. The apparatus of claim 49, wherein the value X is computed according to $X = f(P, F)$, wherein $f(P, F)$ is a reversible function such that $f(f(P, F), F) = P$

55. The apparatus of claim 54, wherein $f(P, F)$ comprises P XOR F.

56. The apparatus of claim 49, wherein the value X is further computed at least in part from a user identifier U.

57. The apparatus of claim 56, wherein the value X is computed according to $X = f(P, U, F)$, wherein $f(P, U, F)$ is a reversible function such that $f(f(P, U, F), U, F) = P$.

58. The apparatus of claim 57, wherein $f(\mathrm{P},\mathrm{U},\mathrm{F})$ is P XOR U XOR F.

59. The apparatus of claim 49, wherein:

the authorizing entity is a host computer communicatively coupleable to the token; and

the value X is stored in the host computer.

60. The apparatus of claim 49, wherein the value X is stored in a memory of the hardware token, and wherein the hardware token further comprises:

means for computing a reference value H associated with the value X; and

means for associably storing the value X and the reference value H in a memory of the token.

61. The apparatus of claim 60, wherein the means for retrieving the value X comprises:

means for computing the reference value H at least in part from the fingerprint F; and

means for retrieving the value X associated with the reference value H.

62. The apparatus of claim 61, wherein the means for computing the reference value H at least in part from the fingerprint F comprises means for computing H as a hash of the fingerprint F.

63. The apparatus of claim 60, wherein the reference value H is computed at least in part from a hash of the fingerprint F.

64. An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:

retrieving a value X from a memory accessible to an authenticating entity, the value X generated from a fingerprint F of the host and an identifier P securing access to the token;

generating the identifier P at least in part from the value X and the fingerprint F; and

transmitting the identifier P to the token.

65. The apparatus of claim 64, wherein the host fingerprint F is computed at least in part from host information C.

66. The apparatus of claim 64, wherein the host fingerprint F is computed at least in part from host information C and a server specific value V.

67. The apparatus of claim 64, wherein the host fingerprint F is computed at least in part from host information C, a server specific value V and a fixed string Z.

68. The apparatus of claim 64, wherein the value X is computed in the token.

69. The apparatus of claim 64, wherein the value X is computed according to $X = f(P,F)$, wherein $f(P,F)$ is a reversible function such that $f(f(P,F),F) = P$

70. The apparatus of claim 69, wherein $f(P,F)$ comprises P XOR F.

71. The apparatus of claim 64, wherein the value X is further computed at least in part from a user identifier U.

72. The apparatus of claim 71, wherein the value X is computed according to $X = f(P,U,F)$, wherein $f(P,U,F)$ is a reversible function such that $f(f(P,U,F),U,F) = P$.

73. The apparatus of claim 72, wherein $f(\mathrm{P}, \mathrm{U}, \mathrm{F})$ is P XOR U XOR F.

74. The apparatus of claim 64, wherein:

the authorizing entity is a host computer communicatively coupleable to the token; and

the value X is stored in the host computer.

75. The apparatus of claim 64, wherein the value X is stored in a memory of the hardware token, and the processing steps further comprise the steps of:

computing a reference value H associated with the value X; and

associably storing the value X and the reference value H in a memory of the token.

76. The apparatus of claim 75, wherein the instructions for retrieving the value X comprise instructions for performing steps comprising the steps of:

computing the reference value H at least in part from the fingerprint F; and

retrieving the value X associated with the reference value H.

77. The apparatus of claim 76, wherein the instructions for computing the reference value H at least in part from the fingerprint F comprises instructions for computing H as a hash of the fingerprint F.

78. The apparatus of claim 75, wherein the reference value H is computed at least in part from a hash of the fingerprint F.